



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/872,659 | 05/31/2001 | David P. Jablon | 155607-0332 | 2773 |

7590 11/24/2004

Phoenix Technologies Ltd.
915 Murphy Ranch Rd.
Milpitas, CA 95035

| |
|----------|
| EXAMINER |
|----------|

NALVEN, ANDREW L

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2134

DATE MAILED: 11/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/872,659

Applicant(s)

JABLON, DAVID

Examiner

Andrew L Nalven

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 May 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17, 19, 20, 22 and 23 is/are rejected.
- 7) ☒ Claim(s) 3, 8, 13, 18, 21 and 24 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>4/5/02</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-24 are pending.

Specification

2. The abstract of the disclosure is objected to because the provided abstract is too long. The recommended length of an abstract is 150 words or less. Correction is required. See MPEP § 608.01(b).

Claim Objections

3. Claims 3, 8, and 13 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 8 recites the limitation "the software" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-4, 6-9, 11-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Ford et al "Server-Assisted Generation of a Strong Secret from a Password."

8. With regards to claims 1, 3, 6, 8, 11, 13, Ford teaches a client computer (Ford, Page 176, Abstract), a network interconnecting the client computer and plurality of authentication servers (Ford, Page 176, Abstract), software running on the client computer and plurality of authentication servers that cooperates to enter a password on the client (Ford, Page 178, column 1 paragraph 2), store a unique random value y_i on each of the servers (Ford, Page 178, column 1 paragraph 2, "Du"), derive a group element P from the password (Ford, Page 178, column 1 paragraph 4 step 1, "P"), send a blinded password value P_x to the servers (Ford, Page 178, column 1 paragraph 4 step 1, "r"), retrieve blinded key shares P_{xy_i} from the servers (Ford, Page 178, column 1 paragraph 4 steps 2-3, "s"), unblind and combine the shares to create a master key K_m (Ford, Page 178, column 1 paragraph 4 step 3, "R" and page 177 column 2 paragraph

Art Unit: 2134

2), and decrypt encrypted private data on the client computer using the master key Km (Ford, page 177 column 1 paragraph 2).

9. With regards to claims 2, 7, 12, Ford teaches the software operating on the client operating to validate the master key (Ford, page 178 column 2 paragraph 2).

10. With regards to claims 4, 9, 14, Ford teaches the software operating on the client operates to decrypt encrypted private data using the validated master key (Ford, page 177 column 1 paragraph 2).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 16, 19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ford et al "Server-Assisted Generation of a Strong Secret from a Password" in view of Coleman US Patent No. 5,717,756.

13. With regards to claims 16, 19, and 22, Ford teaches all that is described above and further teaches the maintaining of a count of bad login attempts (Ford, Page 177, column 1 paragraph 4, some number of failures, page 177 column 2 paragraph 4, number of password hardenings), the number of recent amplifications (Ford, Page 177, column 1 paragraph 4, number of failures, page 177 column 2 paragraph 4), and checking to see if a user account is locked (Ford, Page 177, column 1 paragraph 4, lock

Art Unit: 2134

out). Ford fails to teach the storage of recent Px password amplification request values and a list of timestamps associated with them. Coleman teaches a list of recent values from a client being stored by the server (Coleman, column 9 line 63 – column 10 line 10), and a list of timestamps associated with the list of values on the server (Coleman, column 9 line 63 – column 10 line 10). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Coleman's method of storing values at the server because it increases security by helping prevent replay attacks (Coleman, column 10 line 66 – column 10 line 3).

14. Claims 17, 20, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ford et al "Server-Assisted Generation of a Strong Secret from a Password" and Coleman US Patent No. 5,717,756, as applied to claim 16 above, and further in view of Lipner et al US Patent No. 5,557,346 and Danieli US Patent No. 6,510,513.

15. With regards to claims 17, 20, and 23, Ford as modified teaches the incrementing of the count of bad attempts (Ford, Page 177, column 1 paragraph 4, number of failures). Ford fails to teach the recording of the timestamp, the periodic checking for stale requests, and the deleting of requests. Danieli teaches the recording of a time stamp to note the time when a request was received (Danieli, column 3 lines 16-24). Lipner teaches periodically checking for stale requests that are determined when the difference between any timestamp value and the current time becomes greater than a specific period of time (Lipner, column 14 lines 59-67), and deletes

Art Unit: 2134

corresponding password amplification request values and timestamps (Lipner, column 14 lines 59-67). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Danieli's method of time stamping and Lipner's method of checking for stale requests with Ford as modified because it offers the advantage of ensuring knowledge of the creation time of data (Danieli, column 3 lines 16-24) and ensuring that no secret information survives past its expiration (Lipner, column 14 lines 59-67).

Allowable Subject Matter

16. Claims 5, 10, 15, 18, 21, and 24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

17. The following is a statement of reasons for the indication of allowable subject matter: The cited prior art fails to specifically teach or suggest the sending of the value of Q_a and any prior values of Q_a from earlier runs in the same login session to each server in an encrypted message or the sending of proof of the validated master key (K_m) and each blinded password value P_x to the servers.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Art Unit: 2134

19. Ganesan US Patent No. 5,535,276 discloses an improved system for securing communication using split private key asymmetric cryptography.
20. Thomlinson et al US Patent No. 6,044,155 discloses a method for securely archiving core data secrets.
21. Guthrie et al US Patent No. 6,161,185 discloses a personal authentication system and method for multiple computer platforms.
22. Jablon US Patent No. 6,226,383 discloses cryptographic methods for remote authentication.
23. Connery et al US Patent No. 6,311,276 discloses a secure system for remote management and wake up commands.

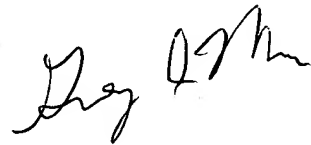
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100